Young
Fraud
Lawyers
Association

Dear All,

Welcome to the YFLA Winter 2024 Newsletter.

Educational and Social Round-up

It was great to see so many of you at the Breakfast and Winter Socials. I think you will agree that both were really well organised and great fun!

The first educational of this membership year will be taking place on 22 January 2025 where we will be joined by a stellar panel to discuss 'A Public Inquiry Into (Anti-)Fraud'. The panel will be chaired by Sir Peter Gross (Court of Appeal, retired) alongside Olga Tocewicz (Hogan Lovells) and Jeremy Brier KC (Essex Court Chambers). Tickets to follow but for now – save the date!

Details of our upcoming events can be found on our website (**www.yfla.com**) and on our LinkedIn group (search for "**Young Fraud Lawyers Association**").

Publicity Secretary's Note

For the first newsletter of the membership year I am delighted to present a bumper edition with eight excellent contributions covering criminal, civil and regulatory developments in the fraud practice area and drawing from the YFLA's solicitor and barrister membership.

- **Philip Gardner and Lauren Stewart: 'Reconsidering Worldwide Freezing Orders: Insights from *Mex Group Worldwide Ltd v Ford & Ors [2024] EWCA Civ 959'***
- **Max Hobbs: 'Modern Slavery: 'Time for a renewed focus?'**
- **James Conroy: 'Prosecution Immunity and the Serious Fraud Office: A double-edged sword?'**
- **Eleanor Turner: 'Financial services and dishonest assistance: Navigating legal responsibilities'**
- **Amelia Clegg and Megan Curzon: 'Nod, nod, wink, wink – The Court of Appeal provides a timely overview of the correct procedure for relying on evidence from assisting offenders'**
- **Daria Solovieva: 'From Compliance to Culture: The Shift in Corporate Governance with the 'Failure to Prevent Fraud' Offence'**
- **Charlotte Branfield: 'The Darker Side to ESG'**

- **Alice Mills: 'Navigating the Future of Tax Enforcement: Insights from the 2024 Autumn Budget'**

I continue to be deeply impressed by the depth and breadth of expertise of the YFLA's membership as illustrated by these articles, and hope that all members will consider volunteering articles for future newsletters.

With sincere thanks to our contributors. Enjoy!

Katie Allard, Publicity Secretary

Reconsidering Worldwide Freezing Orders: Insights from *Mex Group Worldwide Ltd v Ford & Ors [2024] EWCA Civ 959*

Worldwide Freezing Orders (WFOs) are potent legal instruments designed to prevent defendants from dissipating assets, thereby ensuring that potential judgments remain enforceable. Their effectiveness is demonstrated by their applicability to assets both domestically and internationally, making them particularly useful in cross-border disputes.

Despite WFOs being underpinned by well-established principles, the recent Court of Appeal decision in *Mex Group Worldwide Ltd v Ford & Ors* [2024] EWCA Civ 959 has highlighted ongoing complexities concerning their implementation.

Section 25 of the Civil Jurisdiction and Judgments Act 1982 (CCJA)

The Court of Appeal clarified the requirements for granting freezing orders under Section 25 of the CCJA. Notably, it emphasised that a meaningful connection to England is necessary to justify such orders, especially when respondents have no presence or assets in the jurisdiction. The case followed the principle established in *Convoy Collateral Ltd v Broad Idea International Ltd* [2021] UKPC 24, highlighting that an "absence of any assets within the jurisdiction... makes it inexpedient to grant a freezing order."[1]

This position reflects a judicial trend to establish some degree of limit on the use of the English legal system for global enforcement, particularly when orders are ancillary to substantive foreign proceedings where the same relief was available but not granted.

This somewhat more strict approach may burden claimants given the interconnected nature of today's world. Time will tell if historic authorities such as *Credit Suisse Fides Trust SA v Cuoghi* [1998] QB 818, where the court recognised that freezing orders could be necessary even without assets in the jurisdiction, provided it is not "inexpedient" to do so to prevent injustice, will be followed.[2]

---

[1] *Mex Group Worldwide Limited v Ford & Others* [2024] EWCA Civ 959 [110].
[2] *Credit Suisse Fides Trust SA v Cuoghi* [1998] QB 818 [7].

Full and Frank Disclosure

The duty of full and frank disclosure is a long-established requirement for ex-parte applications (see for example the Lady Chief Justice in *Tugushev v Orlov & Ors* [2019] EWHC 2031 (Comm)). In this appellate decision, Coulson LJ reinforced this obligation, warning that non-compliance could lead to the discharge of an order, regardless of its merits. The court found that the claimants' failure to properly disclose material facts was serious enough to justify discharging the WFO.[3]

Nevertheless, Males LJ criticised the respondents' extensive complaints about the claimants' disclosure. He stated, "If the court is presented with a long shopping list of alleged failures of disclosure, with no attempt made to identify the relatively few points which really matter, it should simply decline to consider the issue at all."[4]

Practitioners should take account of this serious warning when giving full and frank disclosure.

Risk of Dissipation

There is considerable debate about how much evidence of general dishonesty should be considered sufficient when assessing a risk of dissipation for a WFO. In *Fundo Soberano de Angola v Dos Santos* [2018] EWHC 2199, Popplewell J (as he then was) stated that "it is not enough to establish a sufficient risk of dissipation merely to establish a good arguable case that the defendant has been guilty of dishonesty; it is necessary to scrutinise the evidence to see whether the dishonesty in question points to the conclusion that assets are likely to be dissipated."[5] This principle was treated somewhat differently in *Mex Group Worldwide*, where the Court of Appeal held that a real risk of dissipation could be inferred from the defendant's dishonest conduct.[6] This was a broader (and claimant-friendly) approach to the test.

In contrast, Charles Hollander KC's decision in *CE Energy DMCC v Ultimate Oil and Gas DMCC* [2024] EWHC 2846 (Comm) reflects a more cautious approach, holding that dishonesty alone does not justify continuing a freezing order without a real risk of dissipation. He stated, "while the defendants' conduct [was] reprehensible, the claimant has not demonstrated a real risk of asset dissipation."

These differing decisions raise questions about which approach should prevail. It seems likely that this might be one of the WFO-related issues that is worthy of yet higher judicial consideration.

Need for Legal Reform?

The Court of Appeal's decision underscores the current complexities and degree of inconsistency in WFO case law. While the judgment reinforces some established

[3] [147].
[4] Ibid [112].
[5] *Fundo Soberano de Angola v Dos Santos* [2018] EWHC 2199 [86].
[6] *Mex Group Worldwide Limited v Ford & Others* [2024] EWCA Civ 959 [66] – [72].

principles, it also adds to the varied precedents in this area which give rise to so many creative arguments on WFO discharge applications. The possibility of statutory reform of the WFO jurisdiction, as hinted at by various judges in recent years, remains a real one.

Philip Gardner and Lauren Stewart
Peters & Peters

Modern Slavery: Time for a renewed focus?

"*When the Modern Slavery Act was passed in 2015, it was said to be world-leading. Since then, the world has changed and best practice has moved on*".

This is the finding of a House of Lords committee report – *The Modern Slavery Act 2015: becoming world-leading again* – that was published on 16 October 2024 (the Report).[7] The Report contains some notable criticisms of the framework and steps currently being taken in the UK to combat modern slavery. It also comes amid some significant recent reporting on cases of modern slavery in the UK and announcements by the Government in this area.

The Report appears to have received little coverage or recognition. However, it contains important analysis of the state of modern slavery in the UK today and recommendations for how the obligations on companies in this area may be strengthened. There is much in the Report for companies to consider, both in terms of their own anti-modern slavery arrangements and how legislation and regulation in this area may change in the future.

The Modern Slavery Act 2015

The Modern Slavery Act 2015 (MSA) introduced, among other things, an obligation under Section 54 on companies or partnerships that carry on business in the UK, which supply goods or services and that have an annual turnover of £36m or more, to publish an annual statement that describes the steps taken by them during that year to mitigate modern slavery risks in their businesses and supply chains. This statement must be published on the firm's website and be approved by the board and signed off by a director (or approved by the members and signed off by the general partner, in the case of a partnership).

While the MSA has been criticised by some for its scope and its effectiveness, it was seen as a landmark piece of legislation when it was introduced. However, the Report is clear that, less than a decade later, the MSA and the UK's approach to combatting modern slavery needs to be revisited. This includes critically assessing the impact of the reporting obligation under Section 54 and calling for it to be strengthened.

The Report

Some of the key points arising from the Report demonstrate the scale and severity of the issue. Among other things, it finds that:

[7] https://committees.parliament.uk/committee/700/modern-slavery-act-2015-committee/news/203272/uks-response-to-modern-slavery-has-not-kept-up-with-the-advances-of-other-nations/

- there are estimated to be around 130,000 victims of modern slavery in the UK (though, it being a "hidden crime" this number may be much larger);
- of the referrals made to the National Referral Mechanism (NRM), only 1.8% result in prosecutions;
- until the current Independent Anti-Slavery Commissioner was appointed (in October 2023) the post had been vacant for 18 months, without explanation; and
- various pieces of recent immigration legislation have limited the protection the MSA provides to modern slavery victims, including by preventing immigration officers from referring certain individuals into the NRM.

Of particular note to companies within the scope of the MSA, the Report has a detailed section on supply chains and the reporting obligation under Section 54. This contains various criticisms of the Section 54 regime, including that it contains little provision for enforcement (and that the existing enforcement mechanism has never been used) and that a hoped-for uptake by companies on a voluntary basis has not materialised.

The Report also highlights the issue that the contents of Section 54 statements are not prescribed or mandated. As the report summarises: "*The contents and quality of business statements appears to be highly variable*". The Report therefore contains various proposals, including:

- prescribing the contents of Section 54 statements, including requiring companies to assess how effective their actions to combat modern slavery have been;
- introducing sanctions for companies that do not comply with their requirements; and
- introducing legislation that requires companies to undertake modern slavery due diligence in their supply chains and take reasonable steps to address any problems identified.

This final point – and the Report's focus on supply chain due diligence in general – is consistent with current trends that can be observed in law, regulation and consumer sentiment. For example, the recent Court of Appeal judgment in the *Uyghur* case[8], relating to money laundering, emphasised the importance of companies understanding their supply chains. It confirmed the possibility of committing money laundering offences by dealing with goods produced by forced labour in a company's supply chain, including where the wrongful activity takes place overseas and even if there has been payment(s) of "adequate consideration" somewhere along the supply chain.

International developments and legislation are also moving quickly in this area and the Report recognises the need for the UK to keep up. Foremost among these developments is the EU's Corporate Sustainability Due Diligence Directive, which will impose supply chain due diligence obligations on large companies that operate in the EU. This, and other international laws, may soon outstrip the MSA. As the Report summarises:
"*The developments internationally on due diligence indicate that the UK has fallen behind. As many UK companies operate internationally, they will find themselves obligated to meet the due diligence requirements of other nations*".

[8] *R (oao World Uyghur Congress) v NCA* [2024] EWCA Civ 715

In these circumstances, political pressure to strengthen the MSA seems likely to increase as time goes on.

Recent examples

The current issues arising in the UK – and the challenges that companies have addressing them – were well-illustrated by recent reports of modern slavery identified at a branch of a prominent fast-food chain and at a food manufacturer that supplied various national supermarkets.[9] In total, 16 vulnerable people worked for several years while the majority of their wages were stolen by a gang and they were forced to live in cramped accommodation.

In particular, various "red flags", which should have raised suspicions, were reportedly missed. These included:

- the wages of the victims were paid into a single account, or into accounts in someone else's name;
- the victims could not speak English – their job applications were completed by other people and a "translator" sat-in on the job interviews;
- the victims worked extreme hours (between 70-100 hours a week); and
- multiple employees had the same registered address. In this case, nine victims lived in a single terraced house.

Companies may wish to consider whether they have the procedures in place that would identify these sorts of common indicators of modern slavery and whether, if such issues were identified, they would be escalated and responded to appropriately within their organisation.

Other announcements

Consistent with the Report, the Government's recent announcements indicate it may be preparing to invest greater focus and resources on this issue. Specifically, on 16 October 2024, Jess Phillips – the Safeguarding minister – announced an intention to "eradicate" a backlog of thousands of modern slavery cases within two years.[10] Among other things, this will involve recruiting up to 200 extra staff. Reportedly, in 2023 there was a record high number of 16,996 potential victims referred to the NRM.

Jess Phillips has also pledged to reform the modern slavery system and increase the number of prosecutions, although it remains to be seen exactly what this will involve. In response to the stories described above, Theresa May – who introduced the MSA – reportedly commented that the MSA now needs to be "*beefed up*".

The Report reminds us that a Modern Slavery Bill (the Bill) was introduced in the 2022 Queen's Speech, although it was not brought forward in the 2022-2023 parliamentary session. The draft Bill contained provisions that strengthened the reporting obligations

[9] https://www.bbc.co.uk/news/articles/c2kdg84zj4wo
[10] https://www.bbc.co.uk/news/articles/c20jg5dj8w7o

under Section 54 and would have introduced civil penalties for non-compliance. It may be the case that the Bill will be revisited, strengthened and brought forward again. In any event, it seems likely that more focus will be placed on this issue in the near future.

Conclusion

It remains to be seen what changes may be made to the MSA and what further steps the government will take in this area. However, the extent of modern slavery is clear; as is the growing expectation that firms should be conducting due diligence on their supply chains to identify and remediate these sorts of issues.

Max Hobbs
Robertson Pugh Associates

Prosecution Immunity and the Serious Fraud Office: A double-edged sword?

Introduction

"There has never been, and never will be, much enthusiasm about a process by which criminals receive lower sentences than they otherwise deserve because they have informed on or given evidence against those who participated in the same or linked crimes. [However,] the stark reality is that without it major criminals who should be convicted and sentenced for offences of the utmost seriousness might, and in many cases, certainly would escape justice."[11]

- Sir Igor Judge, *Blackburn [2007] EWCA Crim 2290, para. 22*

In a recent interview with the Guardian, the Director of the Serious Fraud Office ("DSFO") said that he was interested in utilising the assisting offender ("AO") legislative framework.[12] He was keen on the idea of considering prosecutorial immunity for certain AOs. [13]

It's a bold move. It is right that AOs have the potential to shape and inform the investigation and prosecution of the most serious economic crimes – particularly, in this author's view, cases of international bribery and corruption. However, the use of AOs could exacerbate the biggest issue that has so often plagued the SFO: disclosure. [14]

Immunity from Prosecution: the legal framework

s.71 SOCPA allows the SFO to offer immunity from prosecution to anyone where it thinks it 'appropriate'[15] to do so. The 'immunity notice' that evidences the arrangement, if complied with by the AO[16], precludes proceedings being brought against that AO, except as specified in the notice.[17]

---

[11] *Blackburn [2007] EWCA Crim 2290,* para. 22
[12] s.71/72, Serious Organised Crime and Police Act ("SOCPA") 2005; s.74/388 Sentencing Act 2020
[13] s.71 SOCPA 2005
[14] For more, see the Unaoil review by Sir David Calvert-Smith
[15] s.71(1) SOCPA 2005
[16] s.71(3) SOCPA 2005
[17] s.71(2) SOCPA 2005

The test whether to grant immunity from prosecution was set out by Sir Michael Haver QC (then Attorney-General) in 1981 and has not changed:[18]

i. *"Whether, in the interests of justice, it is of more value to have a suspected person as a witness for the Crown than as a possible defendant;*
ii. *Whether, in the interests of public safety and security, the obtaining of information about the extent and nature of criminal activities is of greater importance than the possible conviction of an individual;*
iii. *whether it is very unlikely that any information could be obtained without an offer of immunity and whether it is also very unlikely that any prosecution could be launched against the person to whom the immunity is offered."*

This is a high bar. Essentially, the SFO will need to ask whether, without the AO, it is very unlikely that it would have the necessary information to bring the prosecution. The old cases where an AO gave 'Queen's Evidence' are illustrative of that high bar. An inside man who had been a part of a conspiracy to commit a serious crime could give evidence of the conspiracy against his co-conspirators. In the days before extensive digital evidence from which the existence of a conspiracy could be proved directly or by inference, this was invaluable. This is a far-cry to a case brought today in which there is extensive digital material. It is hard to see how that high bar test would be made out by an AO who merely directed the SFO to where the best digital evidence may be. Realistically, the best an AO can hope for is a reduction in sentence.[19]

AO Process & Procedure[20]

When investigators are considering utilising AO legislation, a provisional view should be sought from the prosecutor as to its potential suitability. This will require providing the Prosecutor with sufficient information to be able to make that assessment.

After, a scoping interview is arranged. It will examine the kind of evidence/intelligence the AO can provide. They usually occur under caution. However, the AO may also obtain a proffer letter which will establish the "basis and purpose" of the scoping interview before the AO attends.

At this point, authorisation will be sought from the Attorney-General,[21] and a draft agreement will be prepared. That agreement will detail the "terms under which this assistance is to be given, the range of assistance that is to be provided and any benefit to the offender."

Before the agreement is finalised, the AO will need to be 'cleansed' and 'debriefed'. In essence, the AO will need to "admit the full extent of his own criminality,"[22] revealing

[18] https://api.parliament.uk/historic-hansard/written-answers/1981/nov/09/immunity-from-prosecution#S6CV0012P0_19811109_CWA_37
[19] s.74 Sentencing Act 2020
[20] See generally, https://www.cps.gov.uk/legal-guidance/assisting-offenders-immunity-undertakings-and-agreements
[21] This should occur not less than 14 days before the immunity notice is required.
[22] *Blackburn*, para. 27

"the whole of his previous criminal activities."[23] There is also likely to be a requirement that the AO waive his right to legal privilege.[24] The ultimate objective of cleansing and debriefing is for the AO to give "all information available to him regarding the matters under investigation and those involved". In other words, the AO needs to sing like a bird.

The agreement will then be finalised.[25]

Analysis – International Bribery and Corruption ("IBC") cases

It is uncontroversial to say that IBC cases are notoriously hard to investigate and even harder to prosecute.

The highly inferential nature of such cases aside, these investigations often require the assistance of other law enforcement agencies (e.g., the FBI (USA), PNF (France), or others around the world) and requesting evidence via Letters of Request. In some jurisdictions, this will be especially difficult or impossible and the obligation to pursue all reasonable lines of enquiry adds to the burden on English investigators.[26] It is a mammoth task for any organisation, let alone one as under resourced as the SFO.

It is tempting to see the advantage of an AO is these cases if they can provide an evidential nexus to the 'paper' evidence available, through underpinning and tying that inferential evidence together in a narrative told in the first-person. Where activity has taken place overseas and information is not readily available from that jurisdiction, first hand testimony by the AO is obviously especially valuable.

A distinction should be drawn here that the AO is more likely to be considered in a case where there is no cooperating corporate (itself usually seeking a 'deal' via a Deferred Prosecution Agreement ("DPA")) as the two would over overlap such that the high bar test for offering immunity to the AO is likely to fail.

In IBC cases, the nature of the criminality itself needs to be considered. SFO cases are at the most severe end of the white-collar spectrum. They are cases which have been deemed to be of the most severe impact on the public, on the UK's financial reputation and integrity, and on the economic prosperity of the UK itself.[27]

The nature of that criminality needs to be assessed not just domestically. There is also the international knock-on effect of IBC cases, as evidenced through the corporate DPA judgements of the last decade. *Rolls-Royce plc,*[28] for example, concerned corruption across Nigeria, Indonesia, Russia, Thailand, India, China and Malaysia. Applying the Havers criteria, the use of AOs in such cases appears particularly appropriate.

[23] *Blackburn*, para. 40
[24] *Daniels [2010] EWCA Crim 2740*, paras. 60 - 66
[25] For example, see *Blackburn*, para. 7; *Daniels*, para. 35
[26] CPIA Code of Practice 2020, para. 3.5
[27] https://committees.parliament.uk/writtenevidence/107109/pdf/
[28] [2017] 1 WLUK 189

A further thought however is that an AO who is offering evidence of a cross-border offence in exchange for immunity in England and Wales may still be exposed to criminal prosecution overseas.

Disclosure

The disclosure surrounding a long-running investigation, the course of which being informed by an AO, would be substantial. Every decision made by the SFO after the AO had 'come on board', the basis for those decisions and the record-keeping needed to evidence that those decisions would need to be watertight and objectively made.

Moreover, in such large-scale investigations, the cleansing/debriefing process would likely be iterative and long-running. Lines of enquiry would need to be verified, developed and concluded appropriately and in line with the disclosure regime. This in itself could run into the same multi-jurisdictional issues as mentioned above. This would need to occur after every cleansing/debriefing process. Each time this occurs, this provides a potential bullet for the defence's gun. Disclosure would need to be forensic and precise. History would suggest this is not always a given with the SFO.

This risk of disclosure failure in terms of the SFO's investigative obligations would be further stressed as there is a risk of cherry-picked information being fed to the SFO. Granted, it would be a high-risk course of action for the AO (they would be betting their immunity notice on it), but it is nevertheless essential that "the specified prosecutor … be astute to the risk that a professional criminal may be seeking to manipulate the system for his own purposes."[29] Given the previous issues the SFO has had around disclosing information which would assist the defence or undermine the prosecution,[30] a failure to ensure that adequate processes and procedures are in place regarding this would likely (and rightly) attract s.78 PACE 1984 applications.

The disclosure train surrounding the AO may run itself off the rails precisely as a result of the lack of resources at the SFO, rather than seek to ease that lack of resources.

Finally, the risk of being over-reliant on the evidence of an AO in order to secure convictions is high. If defence counsel can exclude the evidence under s.78 PACE 1984, this would leave the SFO in a highly problematic situation. The evidence they have gathered, guided by the information provided by the AO throughout the scoping/cleansing/debriefing processes, would be disconnected from their evidential nexus. The case would become just as inferential as it was before, with no way to tie it together, and with the result that some of that gathered evidence itself be rendered inadmissible under s.78.

Alternatively, the successful challenge to the credibility and reliability of the AO's evidence in cross examination would likely lead to acquittals.

Conclusion

[29] *Blackburn*, para. 31
[30] The prime example being *Akle [2021] EWCA Crim 1879*

Immunity agreements in IBC cases may be the "price worth paying to achieve the overwhelming and recurring public interest that major criminals, in particular, should be caught and prosecuted to conviction."[31] However, the risks are clear and the additional burdens it could place on the SFO may mean that seeking to utilise them would do more harm than good to SFO investigations and prosecutions.

Separately, defence practitioners would do well to be actively involved in AO negotiations from the outset in order manage the process' progression for the best interests of their client. Where it appears this may be an option for a client, defence teams would do well to discuss potential AO agreements early, and engage proactively with the investigation concerning their client to ensure they have the greatest level of control over the process as possible, particularly when proffer letters should be sought. They should also consider potential litigation risk abroad or in parallel civil proceedings.

The terms of the agreement itself – and what the client hopes to get from it (this author posits that, given the DSFO also recently floated paying whistle-blowers, there may be potential room for agreeing that the AO retains some of their proceeds of crime) – should also be carefully considered so that their interests are safeguarded and the agreement remains palatable to all parties. If not necessarily anyone else.

James Conroy
5KBW

Financial services and dishonest assistance: Navigating legal responsibilities

In 2023, fraudsters managed to steal £1.17 billion through both unauthorised and authorised fraud, reflecting a four percent decrease from the previous year[32]. Despite this reduction, there is a consensus amongst authorities that more robust measures are needed to protect consumers.

When trying to recover defrauded assets, victims of fraud often find that the offenders have quickly dispersed the assets. Even with a favourable judgment, the process of asset recovery can be lengthy, costly and ultimately unsuccessful. Consequently, claimants are increasingly seeking to recover losses from those who process fraudulent payments, rather than the perpetrators themselves. This often falls with financial services firms that handle consumer payments and transfers.

The concept of dishonest assistance (a form of secondary liability) has been the subject of significant legal scrutiny and evolution in recent years and claims for dishonest assistance are becoming more prevalent within the financial services sector. However, achieving success in these claims remains challenging, particularly in the context of Authorised Push Payment (*APP*) fraud.

What is dishonest assistance?

[31] *Blackburn,* para. 22
[32] UK Finance. (2024, June 3). Fraud remains a major problem as over £1 billion is stolen by criminals in 2023. Retrieved from https://www.ukfinance.org.uk/news-and-insight/press-release/fraud-remains-major-problem-over-ps1-billion-stolen-criminals-in

Dishonest assistance occurs when a third party assists in the breach of a fiduciary duty committed by another, with knowledge of that breach. The three elements are i) the primary wrongdoer's breach; ii) the assistant's involvement; and iii) the requirement for dishonesty[33]. When dishonest assistance is proven, the defendant is treated as trustee and will be required to compensate the trust for any losses resulting from their dishonest assistance or account for any profits gained.

This form of secondary liability is grounded in the principle that individuals who knowingly assist in the breach of a fiduciary duty should be held jointly and severally liable for the breach. What constitutes dishonest has been found as 'failing to act as an honest person would in comparable circumstances'. The assessment for dishonesty is objective but considers the actual knowledge of the defendant at the time, rather than what a reasonable person would have known or understood[34]. When applying this test in the context of payment providers, a provider will only have acted dishonestly if one of its directors or a person who is deemed 'the controlling mind of the company' acted dishonestly.

Recent claims for dishonest assistance have increasingly arisen in contexts where claimants seek to recover losses from third parties due to APP fraud. APP fraud is a type of financial scam where fraud actors trick individuals or businesses into transferring money under false pretences. This type of fraud often involves criminals posing as legitimate entities, such as banks or government bodies, to gain the victim's trust.

Obligations on payment service providers

In last year's judgment of *Philipp v Barclays Bank UK PLC*[35], the Supreme Court clarified that a bank's Quincecare duty does not extend to payments unequivocally authorised by the customer. In this case, Dr and Mrs Philipp fell victim to APP fraud, instructing Barclays to transfer a large sum to a non-UK bank account. When the funds were lost, they sought compensation from Barclays, arguing that the Quincecare duty or a general duty of care applied. The Supreme Court rejected this claim, stating that the fraudulent inducement of their payment instruction did not invalidate it or create a claim against Barclays. However, the judgment did leave open the possibility for alternative claims for victims of APP fraud.

A claim for dishonest assistance is not confined to parties involved in the initial breach; rather, it encompasses all parties who knowingly participated in the ongoing misappropriation of funds. The recent case of *Larsson v Revolut Ltd*[36] is the latest in a series of decisions addressing the responsibilities of receiving banks, where a customer of a sending bank falls victim to APP fraud. In this instance, Mr Larsson was deceived into transferring funds via SWIFT from his UBS account to various Revolut accounts set up by fraudsters. He alleged that Revolut had failed to implement adequate fraud-prevention measures. Mr Larsson argued that Revolut owed him certain contractual or

[33] Iranian Offshore v Dean Investment [2019] EWHC 472 (Comm)
[34] Royal Brunei Airlines Sdn Bhd v Tan [1995] 3 All ER 97
[35] Philipp v Barclays Bank UK PLC [2023] UKSC 25
[36] Larsson v Revolut Ltd [2024] EWHC 1287 (Ch)

tortious duties as the receiving payment provider and separately to him as a customer of Revolut (despite his Revolut account not being involved in the fraudulent transfers).

For a successful dishonest assistance claim, it is necessary to establish the existence of a trust. Mr Larsson argued that funds transferred through fraud constitute trust property, or alternatively, that a constructive trust could arise over property transferred by mistake if the recipient was aware of the mistake. The court recognised the consequential impact of this issue and decided that it could not summarily dismiss the possibility of a constructive trust of the transferred funds. The court ultimately found the claim of dishonest assistance to be insufficiently pleaded but allowed Mr Larsson to amend his claim to address the identified deficiencies. However, Mr Larsson may still face difficulties in identifying a Revolut representative whose actions meet the threshold of dishonesty, even if he can establish the elements of trust and assistance.

An alternative?

As dishonest assistance claims have yet to achieve success, victims of APP fraud have sought alternative legal remedies against banks and payment service providers. These include claims under the Quincecare duty, unjust enrichment, the retrieval duty, and knowing receipt, each of which has met with varying degrees of success.

One example is the case of *Terna Energy Trading doo v Revolut Limited*[37], in which €700,000 was transferred under an invoice scam to an account held at Revolut, where the funds were then dispersed. The claimant in this case argued that the receiving bank had been unjustly enriched. The court held that there was a real prospect of the claimant proving that the receiving bank had been enriched at the expense of the claimant and therefore denied Revolut's application for summary judgment. In this case, Revolut has been granted permission to appeal.

Another recent example of such claims is *CCP Graduate School Ltd v National Westminster Bank Plc*[38] where the claimant alleged that the sending bank had breached its Quincecare duty and that the receiving bank had breached its duty to prevent accounts being used to transfer defrauded funds. In particular, the claimant argued that both banks owed a retrieval duty and that once on notice of the suspected fraud, the banks were under an obligation to take reasonable steps to recover the assets paid out as a result of the fraud. The court reaffirmed the position established in *Philipp* that the Quincecare duty does not extend to claims involving APP fraud. Regarding the retrieval duty, it acknowledged the "*uncertainty as to whether any such duty lies on the bank of those who can be assumed to have perpetrated the fraud*" (para. 80).

The scope of the expanding duties imposed on payment service providers remains uncertain, necessitating further judicial commentary to clarify claims such as those under unjust enrichment and the retrieval duty. Until such clarity is provided, payment providers and banks must remain attentive to these litigation risks, which may involve substantial obligations that could prove challenging to discharge.

[37] Terna Energy Trading doo v Revolut Limited [2024] EWHC 1419 (Comm)
[38] CCP Graduate School Ltd v National Westminster Bank Plc [2024] EWHC 581 (KB)

Regulatory landscape

Where victims of fraud are left without satisfactory legal recourse, regulators often provide redress to consumers. Last year's Supreme Court decision to deny Quincecare protection to APP fraud victims appears to have been influenced by the upcoming regulatory measures from the Payment Systems Regulator's Mandatory Reimbursement Scheme. The scheme has a claim cap of £85,000 and is designed to provide a safety net for individuals, micro-enterprises and charities affected by APP fraud. However, the scheme excludes non-domestic payments and fraud pre-dating the implementation of the scheme.

Going forward, regulators must balance the need for robust enforcement with the risk of being overly restrictive on innovation in financial services. As the Chancellor of the Exchequer recently encouraged sensible risk-taking within the City, regulators and regulated firms are tasked with necessitating a nuanced approach that can balance the dual requirements of innovation and fraud prevention.

For the regulators, this requires a comprehensive and coordinated approach to both enforcement and redress. This will likely involve collaboration between regulatory bodies, financial institutions and law enforcement agencies. We have seen such a co-ordinated approach in the *London Capital & Finance PLC and others v Michael Andrew Thomson and others* [2024] EWHC 2894 (Ch) case, regarding the criminal prosecution of defendants in conjuncture with the civil claims. It is expected that these levels of regulatory coordination will continue in the coming years.

Conclusion

The financial services sector plays a crucial role in combating fraud. In 2024, banks successfully used security systems to prevent over £1.25 billion in unauthorised fraud payments[39]. However, banks and financial institutions are increasingly facing claims related to their role in facilitating payments. The future of dishonest assistance is likely to see further legal developments aimed at closing existing gaps and addressing emerging issues. Consequently, banks and payment providers will need to prepare for new claims related to fraud losses, driven by evolving legal standards and a greater willingness among victims to seek compensation.

Eleanor Turner
Freshfields

Nod, nod, wink, wink – The Court of Appeal provides a timely overview of the correct procedure for relying on evidence from assisting offenders

I. Introduction

[39] UK Finance. (2024, June 3). Fraud remains a major problem as over £1 billion is stolen by criminals in 2023. Retrieved from https://www.ukfinance.org.uk/news-and-insight/press-release/fraud-remains-major-problem-over-ps1-billion-stolen-criminals-in

The Court of Appeal recently provided guidance on the proper and established procedure for prosecution authorities seeking to rely on evidence provided by an assisting offender. In *R v. Hutchinson* [2024] EWCA Crim 997, the Court considered an application to appeal against a conviction of murder and conspiracy to commit robbery on the basis that the CPS had departed from "*proper and established procedure*" in calling an accomplice as a prosecution witness whilst the same individual was co-accused of murder. The Court expressed its hope that the guidance in this decision would prevent a repetition of the CPS failings in this case, which were "*a matter of serious concern*". Despite the subject matter of this decision, it is a case to note for those practising in business and corporate crime. Given the SFO's commitment to using all tools at its disposal (including paying whistle-blowers and offering immunity), this is an opportune time for lawyers involved in fraud, bribery and corruption cases to review the statutory provisions and guidance from the Court of Appeal which relate to accomplice evidence.

II. Factual Background

Hutchinson (the appellant) and Pycroft were jointly charged with murder and conspiracy to commit robbery following the death of Mihai Dobre in April 2022. Dobre was a drug dealer who had driven his car to meet with what he believed was a prospective customer, just after midnight on 13 April 2022. When he arrived, Hutchinson and Pycroft approached the car. Pycroft then engaged Dobre in conversation whilst Hutchinson - who was carrying a shotgun - walked towards the back of the car and put on gloves, a mask and a hood. Dobre sensed that something was wrong and started to drive away. As he did so, Hutchinson fired the gun through the rear driver's side window, hitting Dobre in the back of the head. Dobre died in hospital some hours later.

III. Procedural History

Both Hutchinson and Pycroft were charged with, *inter alia*, murder and conspiracy to rob. Pycroft subsequently entered into discussions with the CPS inquiring whether the Crown would consider not proceeding with the murder count again him, if he were to plead guilty to the robbery charge and give evidence against Hutchinson.

A. Pycroft's section 74 agreement

Pycroft entered into an agreement with the CPS under section 74 of the Sentencing Act 2020, under which his assistance to the prosecution would be taken into account when determining his sentence. The agreement confirmed that Pycroft would undertake during the required cleansing and debriefing process (outlined below) "*to fully admit and to give a truthful account of his own involvement*" in matters under investigation, including his involvement in the murder of Mihai Dobre [26]. Crucially, the agreement was finalised before the cleansing and debriefing process was complete, and it did not address the murder charge against Pycroft, which still lay on the joint indictment. In other words, Pycroft would not learn whether he would still be prosecuted for murder until after he had given evidence against Hutchinson.

At a mention, Pycroft pleaded guilty to conspiracy to commit robbery before the trial, and although he was still jointly named on the murder count on the indictment, the Crown indicated that it would not try Pycroft for murder at Hutchinson's trial. Noting

that it was the prosecution's intention to call Pycroft as a witness, the judge (who was not the judge presiding over Hutchinson's trial) directed that the section 74 agreement be disclosed to the defence. This was not complied with before trial commenced.

B. Trial

The trial against Hutchinson began on 11 January 2023 before HHJ Enright. Between 10 and 23 January 2023 the Crown disclosed Pycroft's scoping, debriefing and cleansing interviews; the record of his previous convictions; the schedule of offences to be taken into consideration; correspondence between the Crown and Pycroft's solicitors, and other relevant material held by Pycroft's solicitors. Hutchinson's defence team were also permitted to inspect the section 74 agreement[40]. The Crown refused to revisit its position with respect to whether Pycroft would be prosecuted for murder, such that on the day that Pycroft was due to give evidence, one count of murder still lay against him on the joint indictment.

The defence threatened to stay proceedings as an abuse of process on the basis that the Crown's deliberate decision not to resolve the outstanding charge of murder against Pycroft before he gave evidence was a failure to follow proper procedure (in particular as set out in *R v Pipe* (1967) 51 Cr App R 17). The Crown maintained that it had followed the appropriate procedure, but the trial judge warned the Crown that if it did not resolve the position regarding the charge of murder against Pycroft, Pycroft's evidence may be excluded under section 78 of the Police and Criminal Evidence Act 1984. The Crown, having considered its position further, decided to offer no evidence against Pycroft in relation to the murder charge and undertook to not prosecute Pycroft for manslaughter[41]. The Court then rendered a not guilty verdict in relation to the murder charge against Pycroft.

Pycroft was called to give evidence as a witness for the Crown the following day. In his summing-up to the jury, the judge emphasised Pycroft's potential unreliability as a witness, and addressed the reasons why he would be incentivised to tailor his evidence. Hutchinson was nevertheless unanimously convicted of murder.

C. Appeal

Hutchinson appealed on the grounds that the Crown had essentially granted Pycroft immunity from prosecution "*by a nod and a wink*" rather than following the established procedures introduced by statute and set out under the Code for Crown Prosecutors ("**the Code**"), and consequently Hutchinson's defence was prejudiced to the extent that his conviction was unsafe [43]. In particular, it was argued that Pycroft had a strong incentive to give an account implicating Hutchinson and exonerating himself, which made his evidence inherently unreliable such that it could not be fairly admitted as evidence (notwithstanding that the charges were dropped against Pycroft last minute). Counsel for Hutchinson contended that the correct procedures were designed to ensure

[40] The Court of Appeal was critical of the Crown's non-compliance with the directions and general failure to disclose relevant material to the defence, noting that "*these steps should have been taken much sooner, irrespective of whether there was a Court Order*" [35]. Ultimately, the failure was considered to be serious but not deliberate.
[41] This is notable because Pycroft's own evidence indicated that the Crown had a strong case of manslaughter against him, and there was a case to answer that he was guilty of murder as an accessory.

transparency and accountability, and that the Crown had conflated what should have been entirely separate considerations, namely, (a) whether Pycroft's offer to plead guilty to a lesser offence should be accepted, and (b) whether, in return for assisting the prosecution, he should be given a reduction in sentence as a result of his cooperation. It was also argued that excluding the evidence would not have caused any unfairness to the prosecution, and that the prejudice to Hutchinson was not remedied despite the directions given to the jury.

D. Decision – "more pragmatic than principled"

The Court of Appeal denied the appeal, reasoning that although "*there may be cases where no directions to the jury could possibly suffice to cure the prejudice…this was not one of them.*" The Court stated that "*because of the directions given by the trial judge, the jury in this case knew that Pycroft had come forward to give his account at a time when there was no guarantee that he would not continue to be prosecuted for the murder, at which he was now prepared to admit he was present*", and as such the jury was able to assess Pycroft's credibility and motivation [77]. The Court further observed that even if Pycroft's evidence had been wholly discounted by the jury, there was sufficient evidence on which a properly directed jury could be sure that Hutchinson was guilty of murder – Pycroft's evidence was not essential to the Crown's case. Accordingly, the conviction was "*undoubtedly safe*" [79]. Nevertheless, the Court was critical of the Crown's conduct with respect to Pycroft's evidence and stated that "*the failings by the prosecution in this case are a matter for serious concern*" [3]. It added that the decision about the murder charge had to be taken under extreme time pressure and on the face of it appeared "*more pragmatic than principled*", such that Pycroft could "*consider himself extremely fortunate that he ended up in the position that he did*" [72].

Legislative framework for assistance

A. Prosecutorial powers to assist with securing evidence

Prosecuting authorities have the ability to grant the following to assisting offenders, in order to obtain intelligence or evidence which might assist in an investigation or prosecution:

i) Immunity from prosecution under section 71 of the Serious Organised Crime and Police Act 2005 (**SOCPA**);
ii) Restricted use undertakings under section 72 of SOCPA;
iii) Reduction in sentence under section 74 of the Sentencing Act 2020 (previously section 73 of SOCPA[42]); and
iv) Review of sentence under s.388 of the Sentencing Act.

The Crown Prosecution Service's guidance, "Assisting Offenders (Immunity, Undertakings and Agreements)" (dated 2 August 2022) ("**the Guidance**") particularises how prosecutors can use these powers.

[42]The Sentencing Act 2020 repealed and replaced sections 73, 74 and 75 of SOCPA, and takes effect for individuals convicted on or after 1 December 2020.

B. Immunity

Section 71 of SOCPA permits the issue of an immunity notice by a prosecutor (i.e. the DPP or a prosecutor designated by the DPP). The Guidance makes it clear that full immunity will only be granted in the most exceptional cases and specific criteria need to be considered when determining whether it is appropriate to grant immunity to a witness[43]. These include whether, in the interests of justice, it is of more value to have a suspected person as a witness for the Crown rather than as a possible defendant and whether it is unlikely that any prosecution could be launched against the person to whom immunity is offered.

C. Reduction in sentence

Under section 74 of the Sentencing Act, the Court may consider the assistance given or offered by an individual when determining what sentence to pass. Section 74 is engaged where an offender: (i) pleads guilty to an offence; (ii) is convicted in the Crown Court or committed to the Crown Court for sentence; and (iii) has assisted or offered to assist the investigator or a prosecutor in relation to that (or any other) offence pursuant to a written agreement.

The Guidance requires the prosecutor to consider whether an agreement would be acceptable in principle, after which the prosecutor may conduct a scoping interview (usually conducted under caution). The Guidance also notes that, where it is expected that any agreement would include the assisting offender giving evidence in court, an agreement to provide evidence should not be finalised until the offender has admitted their criminality in full under caution ("cleansing") and a full debriefing has been completed. Notably, in the case of *Hutchinson*, this part of the Guidance was not properly complied with.

D. Guidance in *R v Hutchinson*

The Court of Appeal provided several useful observations on the proper procedure for prosecutors to follow when considering accomplice evidence:

First, the Court noted that when a prosecutor is considering whether to accept a defendant's offer to plead guilty to a lesser offence, the primary consideration is whether the plea offered is "*commensurate to the seriousness of the alleged offending*" [65], as well as other factors set out in the Guidance (such as the public interest in the prosecution of and conviction of offenders for the commission of serious criminal offences).

Second, the prosecuting authority may not adopt a "wait and see" approach (as it did in *Hutchinson*) under which it enters into a section 74 agreement with an accomplice and relies on them as a witness against their co-defendant while the accomplice-witness remains charged with the same offence – such an approach is "*wholly impermissible*" [69].

[43]See, in particular, the Attorney General's written answer to the House of Commons on 9 November 1981 (cited as 8 November 1981 in the judgment).

Third, with respect to immunity, the Court of Appeal noted that, although it is not stated explicitly, the language of section 71 of SOCPA envisages that an immunity notice should be considered "***only if*** *the offender has not yet been charged with the offence or offences in respect of which immunity is sought*" (emphasis added) [16]. If the offender has been charged, is willing to admit his guilt, and wishes to give assistance to the police or prosecution in return for a reduction in sentence, then the prosecuting authority should proceed by formalising an agreement with the witness under section 74 of the Sentencing Act.

IV. The impact for fraud lawyers

The guidance provided by the Court, in particular in relation to section 74 agreements, is of relevance to assisting offenders and those being prosecuted on the basis of evidence provided by assisting offenders. Whilst the appeal in *Hutchinson* was unsuccessful, the Court was clear that there may be circumstances where prosecutorial failings of this type cannot be cured by directions to the jury at trial.

Assisting offenders are known to have enabled prosecutions by the SFO in recent years. Many will be familiar with the *Petrofac* case, in which the group's head of sales, David Lufkin, entered into a co-operation agreement with the SFO[44]. His evidence is said to have facilitated a guilty plea by the company in respect of counts under Section 7 of the Bribery Act 2010, resulting in an order to pay £77 million in fines, confiscation and SFO costs[45].

Earlier this year, Nick Ephgrave QPM, the current Director of the Serious Fraud Office ("**SFO**") also confirmed in an interview with The Guardian that the SFO has previously granted immunity from prosecution to an individual who provided substantial assistance[46]. Looking forward, Mr. Ephgrave stated that he intends to bring his experience in "*progressing investigations in all sorts of different ways*" by "*introducing new tactics, new methodologies*" to the SFO. Mr. Ephgrave has identified several "*new tactics*" including offering financial compensation to "*clean hands*" whistle-blowers[47] and possibly granting immunity to suspects or defendants (although Mr. Ephgrave was quick to stress that "*rarely, rarely, rarely do we ever do it*"). Whilst these powers are not new in and of themselves, it is a signal that the SFO intends to bring a fresh approach to the way that these tools are used by prosecutors. It is therefore helpful to have in mind at an early stage of any investigation the applicable legislative framework for assistance and the new Court of Appeal guidance in *Hutchinson,* in anticipation of the SFO's "*new tactics*".

Megan Curzon & Amelia Clegg
BCL Solicitors LLP

---

[44] It is reported that he entered into an agreement under section 73 of SOCPA, which has now been superseded by section 74 of the Sentencing Act.
[45] https://www.gov.uk/sfo-cases/petrofac-limited.
[46] https://www.theguardian.com/law/2024/oct/22/i-can-grant-immunity-from-prosecution-uks-chief-fraudbuster-on-modernising-the-sfo
[47] https://www.thetimes.com/uk/crime/article/corporate-fraud-whistleblowers-could-receive-millions-pounds-53v3dh8bm

From Compliance to Culture: The Shift in Corporate Governance with the 'Failure to Prevent Fraud' Offence

On 6 November 2024, the UK Government released a long-anticipated statutory guidance of the new corporate offence of 'failure to prevent fraud', set to take effect on 1 September 2025 (the "**Guidance**"). This development marks a significant shift in the landscape of corporate crime legislation in the UK, poised to reshape how organisations manage fraud risk and uphold ethical standards.

The Legal Framework

The new offence is rooted in the Economic Crime and Corporate Transparency Act 2023 (the "**ECCTA**") and builds on the existing frameworks established by the Bribery Act 2010 and the Criminal Finances Act 2017. It aims to simplify the prosecution of companies for fraud committed by 'associated persons', fostering a cultural shift towards more robust fraud prevention measures within corporate structures.

Scope of the Offence and Who Is Affected?

Under Section 199 of ECCTA, companies will be criminally liable if an 'associated person' commits a base fraud offence intending to benefit the organisation or any recipient of its services. The term 'associated persons' includes employees, agents, and subsidiaries, while explicitly excluding external service providers like lawyers and suppliers of goods. The legislation primarily targets large organisations, defined by specific employee and financial thresholds. However, smaller firms may also be impacted as 'associated persons' to larger entities, necessitating that all businesses, regardless of size, evaluate their exposure to fraud risk.

Importantly, the legislation applies to both UK-based organisations and foreign entities where *"one of the acts which was part of the underlying fraud took place in the UK or that the gain or loss occurred in the UK." (Guidance for the offence of failure to prevent fraud, 2.5)* . As a result, non-UK companies may face prosecution if fraud occurs in the UK or if UK victims are targeted, regardless of where the organisation is based.

Organisations will have a defence against prosecution by demonstrating that they had 'reasonable fraud prevention procedures' in place when the fraud occurred. Additionally, a company will not be culpable if it is the target or victim of the intended fraud.

Key Aspects of the Guidance

1. **Associated Persons**: The guidance clarifies the definition of 'associated person', emphasising that organisations must establish robust fraud prevention measures across all tiers, including employees, agents, and subsidiaries. Organisations may be prosecuted even if the associated individual has not been charged or convicted of a fraud offence.

2. **Territoriality**: The guidance specifies that the offence pertains to actions with a UK nexus, ensuring that organisations operating internationally are fully aware of their responsibilities under UK law.

3. **Reasonable Fraud Prevention Procedures** The guidance outlines six principles for a comprehensive fraud prevention framework. Organisations must adopt a proactive stance with top-level commitment, incorporating rigorous risk assessments, proportionate risk-based prevention procedures, extensive training programs, due diligence, and ongoing monitoring and review. These principles provide a blueprint for effective compliance strategies, emphasising regular evaluations of fraud risks and the efficacy of existing prevention measures.

4. **Sector-Specific Guidance**: While the guidance applies broadly, it allows sectors to develop tailored strategies that address their unique risks.

5. **Subsidiaries** Organisations can be held accountable if a subsidiary commits fraud intended to benefit the parent company or its clients. Even if the subsidiary is not classified as a large organisation, it can incur liability if an employee commits a relevant offence.

6. **Benefit** Accountability hinges on who benefits from the offence, whether direct or indirect, actual or intended, extending beyond the organisation to its clients or subsidiaries.

7. **Implications for Corporate Ethics** The guidance conveys a strong expectation that organisations must treat fraud prevention with utmost seriousness. The potential for significant legal repercussions underscores the necessity for a cultural shift within companies, prioritising ethical practices and transparency. Companies should remain vigilant in areas vulnerable to fraud, such as misleading marketing practices that could be construed as greenwashing.

8. **Whistleblowing:** The importance of robust whistleblowing mechanisms is emphasised, with recommendations for board-level accountability to oversee such programs.

Preparing for the Change

As the transition period unfolds, organisations should seize the opportunity to bolster their fraud prevention frameworks. A thorough risk assessment can help identify vulnerabilities, enabling companies to implement tailored measures that align with the new legal requirements.

The ‘failure to prevent fraud’ offence represents a watershed moment for corporate governance in the UK. By fostering a culture of accountability and proactive fraud prevention, organisations can ensure compliance with the law while enhancing their reputations and building trust with stakeholders. As the September 2025 deadline

approaches, the call to action is clear: prepare now to safeguard against future fraud risks.

Daria Solovieva

The Darker Side to ESG

Eight years ago in Brussels, as Citigroup/Citibank's global head of government affairs for non-financial risks, I led a discussion on the need for a multi-sector task force on Sustainable Finance with representatives from other financial institutions, credit ratings agencies and corporate firms. It was clear to all from the previous 18 months of regulatory development in the EU[48] and the creation of the Task Force on Climate Related Financial Disclosures, that issues related to the environment and a firm's "social licence" to do business would morph into significant risks.

It was also apparent that the topics I covered – green finance, financial crime, cyber security and data protection – would inevitably converge, a view supported by a report[49] from the UN and Interpol which found that 84% of countries were documenting substantial linkages between environmental crime and other serious crimes. However, it was not until the Sixth Anti Money Laundering Directive ("AMLD6") took effect on 19 July 2024, that 'environmental crime' has been explicitly recognised as a predicate offence.

Since then, what has changed?

Bluntly, it has only been relatively recently that the legislative and regulatory conversation on ESG has evolved from "just" sustainable financing and greenwashing, to "financial crime".

Modern slavery aside, it might be said that there has been no requirement for companies to conduct risk assessments or due diligence on ESG related risks. Therefore, financial crime related to ESG has been, controversially, largely 'ignored' (recognising of course, there has been industry collaboration via forums such as United for Wildlife).

What is ESG?

ESG at its most fundamental is viewed as a company's "social licence" to do business. Viewed through the language of the European Union (EU) Taxonomy Regulation, it means a company should "do no significant harm".

Firms can view ESG through three categories:

1. Know your ecosystem i.e., know your client, procurement and wider supply chain beyond third parties.
2. Safeguard your customers and investors i.e., 'consumer harm', scenario analysis, product development and marketing.

[48] EU Circular Economy Action Plan and EU Non-financial Reporting Directive
[49] 2016 report by the United Nations (UN) Environment Programme and INTERPOL, "The Rise of Environmental Crime – A Growing Threat To Natural Resources Peace, Development And Security"

3. Evolve your decision-making i.e., culture, metrics, reporting.

ESG cuts across all three aspects.

The "E" for environment and the "S" for social share thematic overlaps and include: air and water pollution; mitigating climate change; land conversion such as deforestation, or degradation of peatland, savannahs and grassland; illegal fishing, waste disposal, mining, and wildlife and human trafficking; sexual exploitation; smuggling including of migrants; and forced, slave and child labour.

The "S" also includes: equality, diversity and inclusion initiatives; data protection and privacy; responsible use of technology such as artificial intelligence; and companies' approach to "philanthropic efforts" typically through their foundation and charitable arms.

The "G" for governance includes all elements of how a company makes decisions, including: data quality; culture; conduct; product development and approval; understanding of the consequences of decision-making trade-offs; risk management; systems and controls; Operations; disclosure and other internal and external reporting; Board oversight; and relationships with regulators and governments.

ESG and Financial Crime

ESG is both directly and indirectly linked to financial crime.

Direct examples include illegal fishing, illegal waste disposal and human trafficking, of which there will be a range of predicate offences including fraud, money laundering, forced labour, and sanctions evasion.

For example, in 2022, Natural Resources Wales ("NRW") successfully prosecuted Jeff Lane for logging without a licence and for non-compliance with an enforcement order to replant the trees felled. What makes this case notable is NRW's decision to apply for a confiscation order under the Proceeds of Crime Act 2002 ("POCA"), which they successfully made in June 2024; this is the first time money has been confiscated from a landowner under POCA for offences under forestry legislation.

Indirect examples include where there is legal logging with a legal permit to clear the land but tax evasion on profits and bribery of police to supress local community protests.

When considering financial crime related to ESG, companies should consider it in three ways:

1. First, are they themselves doing an illegal act?
2. Second, do they have a client or a supplier engaged in anti-ESG acts in the context of "due diligence", disclosure and reporting obligations.
3. Third, do they have a client or a supplier they know or suspect of engaging in illegal act related to ESG, such that the company (and senior managers) is in breach of anti-money laundering, fraud, bribery, corruption or terrorist financing obligations.

The second and third points are closely intertwined; at their heart is due diligence.

Due Diligence

According to the National Audit Office, as of 2023, there were 90 regulators in the UK, excluding local authorities which sometimes exercise a regulatory function, across all sectors. Given ESG is a government priority, one must assume that those regulators have been directed to assess what powers of enforcement they have to utilise.

For example, in 2018, the year of its creation, the Office for Product Safety & Standards ("OPSS") subjected 13 companies to enforcement action for failure to implement measures to ensure that timber used in their products was not illegally harvested (11 subsequently complied and 2 were prosecuted), under the EU Timber Regulation (now the UK Timber and Timber Products Placing on the Market Regulations, which has the potential for an unlimited fine on summary conviction). Further prosecutions were brought in 2019 and 2024 against the furniture company, Heartlands Furniture (Wholesale) Ltd, and the luxury yacht maker Sunseeker International Limited respectively, both for failures related to due diligence, record keeping and establishing the systems and controls to ascertain if the timber they used was legal.

What does this mean for financial crime?

Keeping to the illegal logging example. According to Europol, the illicit timber trade is the second most lucrative revenue source for organized crime after drug trafficking, generating an estimated USD 7 billion.

Its predicate offences are, amongst others, money laundering, bribery, corruption and fraud.

In the above example, the bank(s) of the luxury yacht company could potentially have been pursued for failings under The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("**AML regulations**"), for failures in risk assessment and customer due diligence, as well as – and one might say most importantly – under POCA because in that case, those banks should have had reasonable suspicion of money laundering given that the company was importing timber illegally from Myanmar despite sanctions.

Beyond the AML regulations and POCA, other UK laws require firms to investigate their supply chain, report on their impact to the environment and society, and identify key risks. For example, the UK Bribery Act 2010, the Companies Act 2006, the FCA's UK Listing Rules and Disclosure Guidance and Transparency Rules, and Alternative Investment Market (AIM) Rules for Companies. The EU's CS3D will require UK companies with a turnover generated in the EU of more than EUR 450 million to detect and address where their operations can have adverse impacts on human rights and the environment. UK companies in the supply chain of an EU company that is in scope of CS3D will also be indirectly.

These requirements pose the question: how to integrate ESG risk factors into financial crime, KYC and third party due diligence?

The first step for firms is to address their data quality and decision-making by integrating various data systems, adopting a firm-wide consistent process and control taxonomy, and embedding ESG across an enterprise risk framework. Firms should assess what data they have, and can enhance to avoid reinventing the wheel. This approach is key for firms to effectively deploy artificial intelligence or other new technology.

The second step for firms is to develop a full end to end supply chain map. Today, most firms do not have a supplier map beyond their third parties, i.e., only direct ("first level") vendors. Without a robust and complete map, firms will be exposed to numerous 'greenwashing', disclosure and reporting rules, for example, under ss.172 or 414C Companies Act 2006, in addition to the AML regulations.

The third step is actually conducting the due diligence and ongoing monitoring. ESG analysis within KYC and third party due diligence is a very blunt tool, with no ESG equivalent of a sanctions, enforcement or PEP list. A large firm in scope of the AML regulations with 2,000 third parties, will not be able to assess their risk nor narrow down their list of suppliers for further due diligence by using "industry" and "country", even if they overlay that analysis with various country risk and corruption perception indices. This is particularly true for instances of trade-based money laundering, where, keeping with the timber example, illegally and legally logged wood are often mixed together.

It is also questionable what value current supplier surveys have in relation to identifying financial crime related to ESG; gone is the day when it would be acceptable to allow a third-party to answer a survey question with "we have a policy". However, the alternative is to engage a third-party auditor for an on-site audit, which is expensive, only provides a "point in time" snapshot and a limited resource. Firms should consider engaging their suppliers, in a group setting or individually, through training, capacity building, staff engagement (which may also promote whistleblowing), and more support for the supplier's management to engage in effective governance and disclosure. Some firms are exploring using voice pattern risk, as they do in insurance, to assess whether an answer to a pointed survey question indicates further investigation is required, i.e., if a person is hesitant, it may be that they are unsure of their answer for some reason (rather than because they are lying).

The same challenges exist for KYC / onboarding and ongoing customer due diligence.

The fourth step relates to what firms often cite as their most important "control": their employees. Educating employees on environmental and social crimes – the E and the S – are vital to achieving the G, namely financial crime detection and prevention. Part of this education needs to include investigation training which is key to monitoring as well as enhanced due diligence and the onboarding (or KYC) of clients and suppliers.

Reasonable Suspicion

The key legal risk for firms within the scope of POCA, is POCA itself. Whilst the underlying due diligence is challenging, the AML Regulations are largely process driven, but POCA is all about 'reasonable suspicion'.

Arguably given the prevalence of environmental and social crime, it could be said that firms could have reasonable suspicion about most of their client and suppliers.

According to *A v SSHD* [2004] EWCA Civ 1123, suspicion is "is a statement of mind by which the person in question thinks that X may be the case", and the following principles are to be noted as to the law:

- 'Suspicion' is not a high threshold and in its ordinary meaning is a state of conjecture or surmise where proof is lacking: 'I suspect but I cannot prove'. Suspicion arises at or near the starting point of an investigation, prima facie proof at the end: *Hussein v Chong Fook Kam* [1970] AC 942.
- The test is concerned not with proof but the existence of grounds (reasons) for so suspecting, and with the reasonableness of those grounds: *Re Assets Recovery Agency (Ex-parte) (Jamaica)* [2015] UKPC 1; [2015] Lloyd's Rep. F.C. 203.
- Suspicion may be founded on assertions that later turn out to be wrong: *Parker v Chief Constable of Essex Polic*e [2019] 1 W.L.R. 2238.
- The court's assessment of whether there is "reasonable cause" for suspicion is objective, whether in the round, it is a suspicion a reasonable person could hold: *NCA v Hussain* [2020] EWHC 432 Admin.

Clearly, with the due diligence challenges firms face, there will be a real risk of money laundering occurring in their upstream (client) and downstream (suppliers) value chain. This not only needs to be addressed in how a firm manage POCA and suspicious activity reporting ("SAR") obligations, but how it details its exposure to financial crime related to ESG in accounts and reports it is required to publish, and any 'green claims'.

Failure to Prevent Faud

Fraud related to ESG is firmly in the sights of the government regulators. In the November 2024 Guidance on the failure to prevent fraud ("FTPF") offence, under the Economic Crime and Corporate Transparency Act 2023, three of the eight fraud examples related to ESG.

Further, the FTPF offence is focused on 'benefit' versus the more traditional focus on fraud as a 'loss' to a company. Financial crime related to ESG and other ESG issues such as 'greenwashing' fit the definition of "benefit" i.e., sourcing cheaper products and mis-selling which leads to more sales.

S

econd, ESG policies and controls are usually global in nature: "ESG" is seen as part of a firm's brand and marketing. In any event, a firm may have a centralised model for operations such as due diligence. Therefore, the parent company of a multinational firm is more likely than not to be prosecuted jointly with its UK subsidiary (or non-UK subsidiary, if there were UK-based victims, for example). This is particularly so given the FTPF Guidance's broad definition of "indirect benefit".

Applying the principles laid down in *Vedanta v Lungowe and Ors.* [2019] UKSC 20, and *Okpabi & Others v Royal Dutch Shell Plc & Another* [2021] UKSC 3, it could also be argued that a parent could, potentially, incur a duty of care to third parties affected by the operations of subsidiary.

Regulatory Engagement and a New Wave of De-Risking

There is no clear view on what "ESG risk factors". The World Wide Fund for Nature in the UK ("WWF-UK") and Themis have developed an Environmental Crimes Financial Toolkit which will help firms as they start to integrate ESG across existing financial crime monitoring and customer due diligence

Firms must plan now for how best to approach internal investigations, engagement with regulators, clients and suppliers, and adapting and improving their systems.

Absent this communication, firms are not going to "get it right", and regulators will not necessarily know the challenges firms face.

An example of the nuance and trade-offs to consider is the case of Tony's Chocolonely. In the year 2021-2022, it reported in its annual "fair report" that it had found 1,701 cases of child labour in its supply chain. The company described this as a positive: it meant they could identify where child labour was happening and take action to address it. The market and public viewed it differently.

However, one might say that Tony's Chocolonely should have been commended, and that any firm that says it does not have an ESG issue in its supply chain is either wrong due to ineffective due diligence, or worse, knowing but not disclosing.

The public response to Tony's Chocolonely may deter other companies from being transparent; the opposite of what governments and regulators intend and require. It may be that going forwards, a company that is transparent about environmental or social crime in its supply chain is not prosecuted under POCA, whereas a company that doesn't disclose is prosecuted for breach of disclosure or reporting requirements, i.e., under Companies Act 2006, as well as POCA. The FCA's principles-based approach to enforcement is important to consider too, for the firms it regulates, given ESG requires companies to be "good corporate citizens".

In this regard, it will be critical for firms to think about their strategy and approach to any ESG-related investigations. Lessons can be taken from Deferred Prosecution Agreements: in *Director of the Serious Fraud Office v. Amec Foster Wheeler Energy Limited* [2021] Lloyd's Rep. F.C. 353, Lord Justice Edis held that there was a moral standard for self-reporting separate from any legal or regulatory requirements: it was a matter of ethical corporate governance in respect of which there was a moral duty on all citizens which extended at least equally to corporations.

Perhaps the biggest risk to ESG-related financial crime is that the liability risk is just too high. The antithesis of ESG would be a similar event to the banks' de-risking of their correspondent banking networks in the wake of anti-money laundering legislation. The

risk for the banks was too high and compliance too costly and complex, therefore they decided to exit certain local banking relationships, with negative impact to those countries. Applying that here, the risk is that many customers and suppliers will face exclusion from the financial market in turn exposing them to greater money laundering and terrorist financing risks.

Conclusion

With USD1 trillion per year by 2030 being sought to tackle climate issues alone, ESG will increasingly attract criminal behaviour. From fraud related to fitting homes with solar panels, to large-scale illegal mining, ESG already is a significant factor in financial crime.

There will of course be concerns with the effectiveness of regulatory supervision and enforcement: there are already too many SARs being filed. But ESG is a buzzword: joint prosecutions and/or parallel proceedings are likely, whether that be FCA and SFO, or some other combination of the 90 regulators in the country. POCA, and in due course, the FTPF offence, is a "ready to go" tool for tackling financial crime related to ESG.

It is therefore critical for firms to make financial crime related to ESG a priority in 2025 because, ready or not, the regulators and law enforcement seem poised to act.

Charlotte Branfield
Three Raymond Buildings

Navigating the Future of Tax Enforcement: Insights from the 2024 Autumn Budget

The Government's highly anticipated Autumn Budget, announced on 30 October 2024, promises to "fix the foundations of the UK economy." Central to this vision is the Government's pledge to implement "the most ambitious ever package to close the tax gap", including by investing £1.4 billion over the next five years to bolster HMRC's enforcement capabilities, with 5,000 additional compliance officers and 1,800 debt management staff to be recruited.

While the Budget offers insights into the new Government's focus on tightening the UK tax system, understanding HMRC's current enforcement landscape—and the challenges it faces—is essential to anticipate how these policies may shape HMRC's enforcement practices moving forward.

The Government's tax enforcement plans

The Budget places a significant focus on enhancing tax compliance and enforcement as part of broader fiscal reforms. Beyond investing in HMRC compliance staff and digitalising reporting processes, several targeted enforcement policies outlined in the Budget aim to address tax fraud, avoidance, and non-compliance.

Tackling non-compliance by advisers and third parties

For example, strong emphasis is placed in the Budget on tackling fraud and non-compliance facilitated by advisers, agents and other third parties. To combat this, the Budget outlines plans to enhance HMRC's powers and improve regulation in the tax advice market:

- **Enhancing HMRC's powers and sanctions against tax adviser facilitated non-compliance** – The government will publish a consultation in early 2025 on options to enhance HMRC's powers and sanctions to take swifter and stronger action against tax advisers who facilitate non-compliance (paragraph 5.25).

- **Strengthening the regulatory framework in the tax advice market** – The government is publishing a summary of responses to the 'Raising standards in the tax advice market: strengthening the regulatory framework and improving registration' consultation and is considering options to strengthen the regulatory framework of the tax advice market (paragraph 5.24).

Combatting marketed tax avoidance

The Budget also targets marketed tax avoidance schemes, which HMRC estimates accounted for £0.5 billion of the tax gap in 2022-23. Upcoming measures potentially include new powers focused on those who own or control promoter organisations and new options to tackle legal professionals behind avoidance schemes:[50]

- **Tackling promoters of marketed tax avoidance** – The government will publish a consultation in early 2025 on a package of measures to tackle promoters of marketed tax avoidance (paragraph 5.36).

- **Tackling tax non-compliance in the umbrella company market** – To tackle the significant levels of tax avoidance and fraud in the umbrella company market, the government will make recruitment agencies responsible for accounting for PAYE on payments made to workers that are supplied via umbrella companies. Where there is no agency, this responsibility will fall to the end client business. This will take effect from April 2026. The measure will protect workers from large, unexpected tax bills caused by unscrupulous behaviour from non-compliant umbrella companies. The government is publishing a policy paper alongside the Budget that provides further information on this measure (paragraph 5.26).

Offshore tax compliance and fraud

[50] https://www.gov.uk/government/publications/autumn-budget-2024-overview-of-tax-legislation-and-rates-ootlar/841ddc37-58e0-4d3f-9b53-123e8903d274#chapter2

The Government also promises to go further to address offshore tax non-compliance and fraud, an area that remains especially difficult to enforce due to the complex structures employed to evade compliance, often spanning multiple jurisdictions.

- **Offshore tax compliance** – The government is committed to tackling offshore non-compliance as part of the ambition to close the tax gap and is committing additional resources, including the scaling up of compliance activity to tackle serious offshore non-compliance including fraud by wealthy customers and intermediaries, corporates they control and other connected entities (paragraph 5.37).

Enhancing existing enforcement tools

The Budget also indicates the Government's commitment to strengthening existing tools and strategies that support HMRC enforcement:

- Strengthening HMRC's scheme for rewarding informants, to encourage reporting of high value tax fraud and avoidance (paragraph 5.35); and

- Increasing collaboration between authorities, such as HMRC, Companies House, and the Insolvency Service (paragraph 5.33).

<u>The current landscape of tax enforcement</u>

In recent years, HMRC has faced increasing criticism for a marked decline in both criminal and civil enforcement of serious tax fraud. For example, HMRC has yet to impose a single fine on corporations pursuant to the 'failure to prevent the facilitation of tax evasion' offences brought in by the Criminal Finances Act 2017 (the "**CFA**"), and it was reported that only 11 prosecutions were brought against individuals for tax fraud in 2022.[51]

However, prosecution statistics must be understood within the context of HMRC's overarching enforcement strategy, which is primarily geared towards raising revenue. Contrast to other enforcement agencies, which prioritise prosecution, HMRC leans heavily on civil resolutions, which provide a lower-risk pathway to revenue recovery. This approach is reflected in HMRC's criminal enforcement policy, with states criminal investigation will be reserved for cases where HMRC needs to send a strong deterrent message or where the conduct involved is such that only a criminal sanction is appropriate.[52]

[51] https://www.thebureauinvestigates.com/stories/2024-01-20/hmrc-charges-no-companies-for-tax-evasion-in-six-years/
[52] https://www.gov.uk/government/publications/criminal-investigation/hmrc-criminal-investigation-policy

Civil enforcement: HMRC's primary focus

To maximise revenue recovery, HMRC employs a broad array of civil powers aimed at transparency and information sharing. For example, the Code of Practice 9 ("**COP9**") process, which is one of the most important tools in HMRC's arsenal, provides individuals suspected of tax fraud with an opportunity to avoid prosecution by cooperating fully and disclosing all relevant information. This process fosters communication and engagement, which is critical to HMRC's revenue-focused approach.

Similarly, account freezing orders ("**AFrOs**") and account forfeiture orders ("**AFOs**"), introduced under the CFA, enable HMRC to apply to freeze and ultimately confiscate funds suspected to be the proceeds of crime. Unlike criminal proceedings, these measures are governed by the civil standard of proof, enabling asset recovery without lengthy prosecutions. Recent data published by RPC shows that HMRC's use of AFOs increased by more than 170% over three years,[53] highlighting the increasing extent to which HMRC relies on civil mechanisms of recovery over prosecution.

Challenges in enforcement

Despite HMRC's focus on civil enforcement, overall enforcement activities have declined. For instance, in 2023-24, the number of HMRC COP8 and COP9 investigations into tax fraud fell to its lowest in six years, with just 480 investigations being conducted compared to 1,091 in 2022-23.[54] A range of systemic and operational challenges contribute to the downward trend in tax enforcement:

- Resource constraints: HMRC's Fraud Investigation Service ("**FIS**"), which handles most COP9 cases, only accounts for around 0.5% of HMRC's total workforce, however sees frequent fluctuations in staff numbers. As a result, HMRC is limited in the caseload it can handle, particularly as fraud becomes increasingly sophisticated and complex.

- Employee turnover and expertise: According to the Financial Times, high turnover rates within HMRC have depleted the pool of experienced investigators. As is often the case with public sector jobs, skilled staff typically leave for the private sector after a few years, with new recruits lacking the requisite experience to handle complex fraud cases.[55]

- Criminal Court backlogs: Delays in the criminal justice system are a significant deterrent for HMRC to pursue criminal prosecutions, making civil enforcement a more attractive option.

[53] https://www.rpclegal.com/press-and-media/account-freezing-orders-jump-more-than-170-percent-in-three-years/
[54] https://www.ft.com/content/35eb7df3-4005-4d0d-b381-ac45f34da4ed
[55] https://www.ft.com/content/35eb7df3-4005-4d0d-b381-ac45f34da4ed

Looking ahead

The new Government's commitment to reform the UK's tax system, underpinned by a £1.4 billion investment to enhance HMRC's capabilities, has the potential to transform the tax enforcement landscape. The recruitment of 5,000 additional compliance staff represents a positive step in tackling tax fraud, avoidance, and non-compliance. However, the interaction of enforcement measures with external factors such as delays in the criminal justice system is likely to continue shaping HMRC's enforcement decisions.

Continued reliance on civil enforcement

HMRC's preference for civil enforcement is unlikely to change. While the resource challenges currently faced by HMRC will be eased by additional funding, a sharp increase in criminal enforcement activity is unlikely. Nevertheless, the Budget states the Government's intention to take "stronger action on the most egregious tax fraud, including by expanding HMRC's criminal investigation work", and so a limited rebalancing of HMRC's approach should be expected.

Corporate prosecutions

As of July 2024, HMRC was investigating 11 cases for the offence of failure to prevent facilitation of tax evasion under the CFA, and had an additional 28 cases "under review." With the Government's focus on offshore compliance, and the potential for these cases to leverage the CFA's extra-territorial provisions, the first corporate prosecution may be imminent.

Additionally, the introduction of the failure to prevent fraud offence under the Economic Crime and Corporate Transparency Act 2023 ("**ECCTA**"), which comes into effect on 1 September 2025, expands HMRC's ability to hold organisations accountable for the offence of cheating the public revenue. While cheating the public revenue is one of the base offences caught by the offence of failure to prevent facilitation of tax evasion in the CFA, the ECCTA covers a wider scope in terms of who can commit the offence.[56]

Enforcement against advisers, agents and promoters

The Budget places significant emphasis on tackling fraud facilitated by advisers and agents. This priority is reflected in recent raids on consultancy firms offering advice on Research & Development ("**R&D**") tax relief, which is a relief designed to enable companies engaged in qualifying R&D to claim tax benefits for eligible expenditures.[57]

[56] https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta/economic-crime-and-corporate-transparency-act-2023-guidance-to-organisations-on-the-offence-of-failure-to-prevent-fraud-accessible-version

[57] https://www.bbc.com/news/articles/cvgl5gw060eo

In its latest published annual accounts, HMRC indicates that over £4bn of its total expenditure on R&D tax relief scheme since 2020/21 was paid out as a result of fraud and error by the taxpayer, signaling the scale of the issue.

Future enforcement will therefore likely continue in this area by combining targeted investigations into advisor-facilitated fraud and marketed tax avoidance with regulatory reforms intended to improve oversight of practitioners and provide additional ways to monitor and enforce minimum standards.[58]

Offshore compliance as a priority

Finally, High Net Worth individuals, the corporations they control and their associated intermediaries are likely to remain a key focus for HMRC. The Government's intention to improve rewards for informants and enhance collaboration between agencies demonstrates its commitment to foster a more coordinated and intelligence-driven approach to tackling tax evasion and fraud. This approach is particularly relevant to addressing the challenges posed by typically impenetrable offshore tax structures. As a result, we can expect HMRC to intensify its targeted enforcement efforts against those evading taxes across jurisdictions.

Conclusion

The Government's commitment to reforming the UK tax system has potential to reshape HMRC enforcement. While civil enforcement will likely remain central to HMRC's revenue-raising strategy, the combination of increased resources, regulatory reforms, and heightened scrutiny indicate a possible shift toward a more balanced approach that includes increased criminal enforcement. These changes signal a stronger, more coordinated effort to combat tax fraud, avoidance, and non-compliance in the coming years.

Alice Mills
Cohen & Gresser (UK) LLP

We would like to extend our heartfelt appreciation to all our contributing authors.

[58] https://www.gov.uk/government/consultations/raising-standards-in-the-tax-advice-market-strengthening-the-regulatory-framework-and-improving-registration/5841a117-9ea5-4311-9524-ff81ef39c998